those circumstances where a customer orders CUSTOMNET (and U S WEST, therefore, transmits ANI 7 digits to identify that special billing is required), not all IXCs/OSPs recognize and/or honor the information provided. For CUSTOMNET to work in a manner that meets customer expectations, the OSP involved in handling the outgoing call must have operator service equipment capable of receiving the transmitted ANI 7 digits and must subscribe to U S WEST's Call Screening Service.[27]

When U S WEST sells CUSTOMNET, we advise customers of the fact that the successful operation of the service depends not just on what they order, but also on the OSP accessed from their station equipment. Most of the larger IXCs/OSPs have appropriate equipment and do subscribe to our Call Screening Service. Thus, CUSTOMNET will work satisfactorily for a customer in most instances. However, this cannot be said for all telecommunications transactions undertaken by CUSTOMNET customers.

U S WEST assumes that, after being advised by U S WEST about the interaction between CUSTOMNET and a customer's chosen carrier, most customers ordering CUSTOMNET probably will choose to presubscribe to an IXC who will honor the transmission of the ANI 7 information sent about them. But some customers, such as call aggregators or payphone providers (who have an obligation to make 10XXX access available),[28] do not have the same level of control

---

[27]When an OSP subscribes to such service, the OSP can translate the ANI 7 digits correctly and can process the billing in conformity with the expressed desire of the end-user customer.

[28]See 47 CFR § 64.704.

as a privately-controlled business operation. Thus, while calls made from the aggregator's CPE through the aggregator's own presubscribed carrier might successfully be controlled through a CUSTOMNET offering, the fact remains that the 10XXX call might well access an OSP who either does not have the equipment to recognize the ANI 7 digits or does not know how to translate them.[29] In such a situation, the expectations of the CUSTOMNET subscriber -- the aggregator -- will be defeated.[30]

Thus, it is clear that CUSTOMNET is not a guaranteeable service offering, depending as it does not only on a customer's expressed intention as to how it wants its toll access controlled, but also on the kind of OSP equipment encountered during the processing of the outgoing call transaction.

(2) Billed Number Screening ("BNS")

This service provides a customer with the capability to restrict incoming collect and/or third-number billed calls.[31] Callers attempting to bill the BNS customer's line number for calls, or to complete a collect call to that line number, are

---

[29]This could happen with a small IXC or OSP operation, for example.

[30]While a direct-dialed call probably could not be completed and would go to an intercept, a regular operator-assisted call billed to the customer's account could be accomplished. The party accessing the OSP via the 10XXX dialing might allege difficulty in completing the call directly and ask for assistance, but not for alternative billing.

[31]In U S WEST's territory, BNS is offered to end users at no charge, except in Minnesota.

intercepted and advised that such billing is unauthorized and that another form of billing is required.

This service will operate successfully on a customer's line only in situations where the carrier/OSP handling the calling party's call subscribes to U S WEST's LIDB, in fact queries LIDB, stays on the line long enough to secure the necessary information, and correctly interprets the response regarding the control features on the called party's line. This is not always the case.

While a number of factors can cause a BNS-requested service not to work,[32] a few are worthy of particular mention. A carrier/OSP has to query LIDB to get the information, and not all carrier/OSPs do.[33] Even when LIDB is queried, sometimes the

---

[32]Human error, for example, in inputting the service order information might cause the information to be entered incorrectly. See also supra note 24.

[33]While the Commission's current NPRM suggests that an OSP might have some "duty" to access LIDB for relevant and material information pertaining to call handling ("If a LEC card is offered for billing, the IXC or . . . (OSP) should query the LIDB to determine whether the card is valid for use.") (NPRM ¶ 36 (emphasis added)), it does not affirmatively state that one exists, nor does it imply that it extends to verification of customer screening services, such as BNS.

While, theoretically, creating or establishing such a duty might not seem difficult or overreaching, the Commission should be aware of certain facts with regard to LIDB access and its "verification." Currently, U S WEST has limited capabilities with regard to tracking access to LIDB. For example, while we can generally tell, by volume, the number of times an individual IXC/OSP has accessed LIDB, we cannot "match" a particular access (i.e., a query) to a particular completed call. Furthermore, there are certain circumstances in which we cannot even verify that a certain IXC/OSP accessed LIDB, at all. For example, when an OSP accesses LIDB via an OSP aggregator, U S WEST does not

(continued...)

carrier/OSP disengages the transaction prior to the time the information is provided to the OSP[34] and billing the customer expressed an interest in not permitting gets completed.[35]

Thus, like CUSTOMNET, BNS is not a guaranteeable service offering. Rather, it is an aid to customers who want some control over the kinds of calls billed to their telephone number. It is not perfect.

c. Calling Card

U S WEST offers a telephone calling card which may be used for intraLATA toll calls; and, if accepted or honored by IXCs or OSPs, can be used to place interLATA and international toll

---

[33](...continued)
know the identify of the specifically-querying OSP -- only the aggregator's identity. Thus, U S WEST would be unable to demonstrate whether a particular OSP accessed, or did not access, LIDB. Similarly, calls originating from international locations are not validated in LIDB unless the overseas operator hands the call off to a domestic carrier who then validates through LIDB. For all these reasons, it would be impossible for U S WEST (from LIDB information) to be able to prove or verify that an IXC/OSP either did or did not perform its "duty."

[34]A LIDB response may be delayed due to network and/or system congestion in either the LEC's or the OSP's network.

[35]While at first glance this may appear to be an absolute breach of the customer's expectation, more facts need to be considered in the equation. For example, while a customer may have asked for BNS (a service which U S WEST currently provides in all our states except Minnesota at no charge), when an OSP places the call and inquires at the premises whether a collect call or third-party billed call will be accepted, someone on that premises has an opportunity to say "yes" or "no." Only if the answer is "yes" will the call be completed. Thus, a reasonable argument can be made that, while the umbrella screening service did not operate as anticipated by the customer, specific authorization for the individual transaction was, in fact, secured, and the customer should be responsible for the attendant charges.

calls. In the material we provide to our customers about our calling card, we identify several important safeguards a consumer can/should follow to alleviate potential fraud. We place this information conspicuously in the material sent to customers about the operation and use of the card.[36] As an additional security precaution, the customer's security code (i.e., the Personal Identification Number ("PIN")) is not embossed on the calling card itself.[37]

2. Services For IXCs and Alternative Carriers

a. LIDB

U S WEST, like other LECs, provides a LIDB for validation of U S WEST calling cards. This system is also able to advise whether a line number will accept third-party/collect calls, and it can do public telephone checks and vacant number checks.

U S WEST constantly monitors the threshold acceptance outputs of LIDB. We maintain a 24-hour, 7-day-a-week fraud investigation unit that continuously assesses the LIDB data integrity and investigates suspicious call activity to detect and deter fraudulent usage. This fraud unit works closely with all LIDB customers, and internally within U S WEST, to keep fraudulent calling to a minimum.

---

[36] See Appendix B hereto.

[37] U S WEST also sponsors a VISA card that can be used as a calling card. The same security information is provided to customers about the use of this card as a calling card as is provided to the traditional calling card customer.

LIDB is not, however, a guarantee against fraud. Carriers are not currently compelled to access LIDB, and U S WEST would not have the ability to determine with accuracy if, in fact, a carrier did access LIDB prior to completing a call or stayed on the line long enough to secure the necessary information.[38]

Additionally, not all possible validation and screening information gets populated in the LIDB query. For example, while U S WEST currently receives calling/called number information from some IXCs/OSPs accessing LIDB, we do not receive such information from all IXCs/OSPs. The inclusion of calling number information in the LIDB query would greatly improve the LECs' fraud detection and prevention efforts by providing information that can be used in identifying unusual usage patterns (i.e. multiple origination points), and in identifying to the card-holder specific calling numbers during the course of an investigation. Additionally, as enhanced fraud control features become available, receipt of the calling/called number in the LIDB query will be used to determine and provide alert notifications to the LIDB provider's fraud investigation unit as described in the following paragraph.

b. Future/Impending Offerings

U S WEST envisions that shortly we will be offering enhanced fraud control features in LIDB (currently called Customized Fraud Management Services ("CFMS")). These features/functions will

---

[38]See supra note 33.

allow LIDB customers to implement customized customer thresholds and tracking mechanisms with regard to calling card, third-party and collect calls in ways that meet their particular business needs. Thus, for example, an IXC will be able to advise U S WEST that upon the happening of event A (e.g., a call coming from multiple originating or going to multiple terminating destinations designated by the carrier as suspicious), event B should occur (e.g., an investigation based on carrier-identified parameters should be initiated).

And, as mentioned above,[39] U S WEST has established an e-mail system that both sends and receives information on toll fraud, which is shared both internally and with interested carriers. We are also currently working with carriers on coordinating and implementing other complementary mechanized systems to allow for the passage of fraud control information, in a more expeditious manner.

c. Billing and Collection-Related Services

Certainly, those products offered to IXCs as IXCs (see discussion above at 2.a and 2.b) aid those same IXCs in the billing and collection of their services. In addition to those offerings, U S WEST works closely and cooperatively with our various carrier customers in analyzing innovative ways to detect fraud through the billing information we are provided, in our agency capacity.

---

[39] See text at pp. 14-15.

Furthermore, as the billing agent for certain IXCs, we attempt to be tenacious in our efforts to collect monies due and owing with regard to fraudulent activities. We also work closely with law enforcement personnel in bringing fraud perpetrators to justice, supporting appropriate arrest and prosecution activities.

In addition, upon carrier request, U S WEST will conduct a fraud control review for a carrier. In such a review, U S WEST will outline our fraud control and prevention program and speak frankly with the carrier about the kinds of things we can do for the carrier and what we expect the carrier to do. In the last quarter of 1993, we conducted two such reviews: one with MCI in October; and a two-day review with Sprint in November, during which time U S WEST personnel visited the Sprint facilities in Kansas City to get a better understanding of the kind of cooperation necessary to better combat fraud problems.

D. Education Efforts

U S WEST is proud of our customer education efforts with regard to fraud. We have developed a fraud brochure that we provide to business customers (see Appendix C hereto), that -- while not dispositive or preemptory -- describes how fraud might occur within/to a business and suggests measures that might/should be taken to protect against such fraud.

The brochure addresses matters on controlling and limiting PBX- and Centrex-remote access capabilities, developing security

access codes (which might require more than expected digits and which need to be frequently changed), monitoring call volumes during weekend, night and holiday hours, and outlining how hackers use voice mailbox systems to perpetrate toll fraud. The brochure also provides details on fraud activities which have been successful and discusses ways in which business customers can implement prevention mechanisms to limit their exposure to those activities.

In addition, as mentioned above, U S WEST provides our calling card customers with information which conspicuously highlights fraud risks and prevention tactics. Similar information is made available to those customers having a U S WEST VISA card which can also be used as a calling card.

U S WEST has also developed a 13-minute videotape entitled "Telecommunications Fraud and You." This video informs the viewer of the potential exposures they might have with toll fraud. It educates the viewer on how a hacker can compromise a PBX-remote access feature, voice mail, and PIN numbers to gain unauthorized access through the customer's CPE to the toll network. Additionally, the video covers the topics of call/sell fraud[40] and subscription fraud, and is used to educate U S WEST internal personnel to the tactics used by fraud experts. This

---

[40]A fraudulent call/sell operation typically involves the ordering of telecommunications services (with no intent to pay for the services) with the intent of selling long distance services for cash payment. Call/sell operators may also resell long distance services accessed through successful PBX hacking efforts or stolen calling cards.

video has been used in numerous customer meetings, at toll fraud seminars U S WEST has sponsored, and in presentations that our security personnel have made to U S WEST's marketing channels.

U S WEST has also conducted numerous fraud seminars over the past five years. In 1993 alone, we held nine of them (in Seattle, Portland, Spokane, Omaha, Phoenix, Cedar Rapids, Des Moines, Minneapolis and Denver). In 1992, we conducted eight others.

In light of the already extensive education efforts conducted by U S WEST (which have been lauded as a model for the industry), and those we know are already being conducted by other carriers (and which can be expected to increase), U S WEST sees no reason, at this time, for the Commission to act in a formal regulatory capacity "to broaden established Commission and industry consumer education initiatives in order to better educate consumers about toll fraud risks and remedial steps that can be taken."[41] While the Commission should certainly acknowledge ongoing industry activities, and should give credit where credit is due, there is no demonstrated need that requires the Commission to act in a compulsory capacity with regard to customer education efforts.

---

[41] NPRM ¶ 13.

III. THE LECS' EXISTING LIMITATION OF LIABILITY PROVISIONS DO NOT ADVERSELY AFFECT SOUND RISK MANAGEMENT PRINCIPLES INVOLVING FRAUD RESPONSIBILITY

A. An Overview of the Problem and the Matter of Liability Limitations

The Commission recognizes that the manner in which fraud responsibility is allocated can affect if, when and how fraud is controlled.[42] As U S WEST discussed in our introduction, we believe that suggestions that carriers bear a more substantial responsibility for fraud losses in an effort to encourage them to become more active in fraud prevention is a theory divorced from the contextual reality of how opportunities for fraud are created.

In most circumstances the opportunity for fraud is created by the vehicle that allows access to the network -- the telecommunications equipment. And, while carriers can devise certain products/services that can operate as aids to customers with regard to what happens once that network access is accomplished, they cannot be expected to be guarantors of those service offerings -- especially to the extent that their successful operation depends on the behavior of various and varying network providers.

But what about those circumstances in which a carrier could have done something more or different? What about those circumstances where the service order did not get correctly input or the carrier disengaged from LIDB prior to the time the screening

---

[42] Id. ¶¶ 24, 41.

information was conveyed? There is a suggestion in the totality of the NPRM that the Commission is disturbed by how current liability principles allocate the loss in such a situation, i.e., the carrier generally bears no responsibility in the absence of gross negligence.[43] This seems unfair or inequitable because, the argument goes, the customer has done all it could. Someone else (i.e., some carrier) should be held responsible.

There are two distinct considerations in addressing the public policy ramifications of the above argument. First, customers who are the subject of fraud as a result of the negligence of a LEC[44] are really in no different situation than

---

[43]NPRM ¶ 39. Such a standard was adopted with the understanding that simple negligence occurs in all businesses; and on the theory that it was a better public policy approach to ask a few individuals to bear the expense of a simple negligent act than build into the rate base assumptions of liability for negligence.

While the concept of "rate base" may retain little remaining viability, the Commission should accord LECs the business discretion to determine when, and for how long, such limitations are necessary. Such limitations are, for example, still used by carriers heavily engaged in the provisioning of competitive services. Indeed, one of the primary reasons that MCI took the Commission to court on its refusal to allow MCI to file tariffs (as a consequence of the Commission's "forbearance" policy) was to establish a tariffed limitation of liability that would apply, as a contractual provision, to its customer relationships. See Brief for Petitioner, MCI Telecommunications Corp., at 8, 70 n.198; Reply Brief for Petitioner, MCI Telecommunications Corp., at 24, 28, No. 85-1030, MCI v. FCC (D.C. Cir. Apr. 1, 1985; May 15, 1985).

[44]U S WEST here addresses the matter of negligence, but it is important to remember that a service might not work simply as the result of a "mistake" -- something not even approaching negligence (such as a mistyped service order).

(continued...)

customers who suffer other kinds of economic losses due to LEC misconduct. In the case of fraud, a customer has to pay the charges for the traffic actually transported; in other cases, a product/service failure will deprive a customer of traffic (either incoming or outgoing) and can "cost" the customer a considerable sum in lost revenue. In both cases, the result can be declared "unfair," but in neither case should it be declared unlawful.[45]

---

[44](...continued)
Certain of the NPRM remarks suggest that a customer should be absolutely immunized from fraud liability in certain circumstances (compare the Florida Public Service Commission ("Florida PSC") proposal, NPRM ¶ 27 n.42), with liability being apportioned among carriers in relation to their responsibility, not necessarily fault. Thus, such proposals would render a carrier absolutely liable for the malfeasance of a service, even in the absence of negligence. And, in all events, a factual determination would be required to determine the source of responsibility, which in and of itself would be very time consuming and might not even be dispositive. See supra note 33, and further discussion below.

[45]It would be extremely difficult, especially in the context of a particular docket, for the Commission to carve out a liability provision for a particular class of customers different from that generally applicable to LEC customers. An idiosyncratic approach to liability is bound to create certain discriminations. And, it cannot be known whether the discriminations are reasonable without looking at the discrimination (and its effects) within the context of the remaining customers, something a particular docket (such as one on fraud) is not in a position to do.

This is not the only proceeding, for example, in which LEC limitations of liability are being challenged. Intervening interconnectors have attacked such provisions within the context of the Expanded Interconnection dockets, as well. See, e.g., In the Matter of U.S. WEST Communications, Inc. Revisions to Tariff F.C.C. No. 1, Transmittal No. 331, Teleport Denver LTD.'s Petition to Reject or, in the Alternative, to Suspend and Investigate Transmittal No. 331, Tariff F.C.C. No. 1, filed Mar. 15, 1993, at 8; In the Matter of U S West Tariff F.C.C. No. 1, Petition of
(continued...)

Second, it will not generally be possible to know that a customer did "all it could" without a fact investigation.[46]

---

[45](...continued)
Sprint Communications Company L.P. to Suspend and Investigate filed Mar. 15, 1993, at 12-14; and In the Matter of The Bell Atlantic Telephone Company Tariff FCC No. 1, et al., Transmittal No. 557 et al., Petition of The Ad Hoc Telecommunications Users Committee to Reject in Part, or Alternatively, Suspend and Investigate, Expanded Interconnection Tariff Revisions, filed Mar. 15, 1993, at 35-38. See also In the Matter of Local Exchange Carriers' Rates, Terms and Conditions for Expanded Interconnection for Special Access, CC Docket No. 93-162, Comments of Direct Cases, Teleport Communication Group Inc., filed Sep. 20, 1993, at B-20 - B-27; and Opposition to Direct Cases, CC Docket No. 93-162, Sprint Communications Company L.P., filed Sep. 20, 1993, at 17-20, Appendix A. As we did there, U S WEST here argues that an exception from traditional LEC limitations of liability should not be created for a single class of customer without addressing the overall matter of liability and liability limitations. See In the Matter of U S WEST Communications, Inc. Revisions to Tariff F.C.C. No. 1, Transmittal No. 331, Reply of U S WEST Communications, Inc., to Petitions to Reject, Suspend and/or Investigate filed Apr. 5, 1993, at vi, 71-72. See also In the Matter of Local Exchange Carriers' Rates, Terms and Conditions for Expanded Interconnection for Special Access, U S WEST Communications, Inc. Revisions to Tariff F.C.C. No. 1, CC Docket No. 93-162, U S WEST Communications, Inc., Rebuttal, filed Oct. 1, 1993, at 57-62.

[46]Compare NPRM ¶ 24, discussing the factual resolution associated with the Chartways and United Artists complaints ("The dispositive element in each of these cases was where responsibility for the detection and prevention of fraudulent calling lay[.]"). See also id. ¶ 39 (where the Commission addresses LIDB fraud, noticing that the "[a]ssignment of liability" may be dependent on "many different fact patterns each time a loss is generated, making the development of a general rule difficult." This is not true just for LIDB fraud, however, but for all kinds of telecommunications fraud.).

Furthermore, establishing rules such as those suggested by the Florida PSC for payphone providers (i.e., that if the provider purchases OLS and BNS, the payphone provider is relieved of all economic responsibility for transactions completed in contravention of the offerings) basically immunizes the payphone provider from any responsibility, in the future, to protect itself through the utilization of more intelligent CPE or other devices that might go a long way to alleviate the problem.

Such investigations are resource intensive, as is demonstrated by the detail associated with the Chartways and United Artists[47] complaints; and do not generally get resolved in a timely fashion. Individual case reviews are not easily aligned with a large bureaucratic organization which operates, at least in the telecommunications field, without the benefit of hearing examiners or fact finders.

Any kind of fault or comparative responsibility approach[48] will require a case-by-case disposition.[49] While the complaint process is moderately suited to such dispositions, it is a cumbersome and time-consuming endeavor. And, the lack of any currently-pronounced methods and procedures associated with the Commission's alternative dispute resolution process makes endorsing it as a more appropriate vehicle difficult.[50] Certainly, parties can be encouraged to proceed to arbitration, but the lack of established policies/principles surrounding it might also render it unattractive, at the moment.

In light of the fact that carrier limitations of liability are not unlawful, and that they currently operate in a

---

[47] In the Matter of Chartways Technologies, Inc., Complainant, v. AT&T Communications, Defendant, Memorandum Opinion and Order, 8 FCC Rcd. 5601 (1993). In the Matter of United Artists Payphone Corporation, Complainant, v. New York Telephone Company, and American Telephone and Telegraph Company, Defendants, Memorandum Opinion and Order, 8 FCC Rcd. 5563 (1993).

[48] See NPRM ¶ 25.

[49] Compare id. ¶ 24.

[50] See id. ¶ 25 (where the Commission requests comment on the possible use of alternative dispute resolution procedures).

nondiscriminatory fashion with regard to all LEC customers, and that their existence clearly does not impede a carrier's concern about fraud prevention or its motivation to be a part of the solution to fraud, the Commission should not intervene to require changes in those liability limitations. If, over time, carriers determine that the marketplace requires some other kind of liability allocation, such will be forthcoming. But, until then, the Commission should refrain from interjecting itself into the risk allocation decisions of the LECs' businesses.

B. Liability for LIDB Failure

The Commission inquires as to whether, in certain circumstances, it might be appropriate to hold the LIDB owner/operator liable for toll losses.[51] LIDB malfunctions should be treated like any other non-working service offering, and should be covered by LECs' existing and standard limitations of liability. In the absence of gross negligence, LECs should not be liable.

The Commission itself acknowledges that the operation of LIDB is only as good as the information put in it, that not all calling card activity gets input to LIDB, that at certain times LIDB is not queried, and so on.[52] Thus, LIDB is more like a "credit reporting" source than a receivables guarantee. Each and every carrier can determine, from the information contained therein, what that carrier will do, given the information

---

[51] Id. ¶ 39.

[52] Id. ¶¶ 37-39.

disclosed. Some carriers are willing to assume more risks than others, and that is something the market should permit.

Operating a system such as LIDB cannot be done with perfection. There are various things that can cause LIDB to give an "incorrect" response, ranging from a clerk who miskeyed information, to a carrier who does not access the system, to a carrier who accesses the system but does not stay on the line long enough to get the information.

Given the recent regulatory history associated with LIDB, the product offering has become as much defined by this Commission as by the LECs themselves. Thus, it would be especially inappropriate for the Commission to convert what was perceived as a tool for fraud prevention into a guaranty against fraud losses. There are no such guarantees, and U S WEST is not willing to establish one for LIDB.[53]

---

[53]In those situations in which U S WEST is fairly confident in the performance of one of its products/services, and believes it is an appropriate candidate for service guarantees, we provide them. See U S WEST Tariff F.C.C. No. 1 Section 2.4.4(B)(11), DS1/DS3/WATS Voice Grade services restoration guarantee or credit. LIDB is not one of those services.

IV. THE RESPONSIBILITY FOR FRAUD PREVENTION AND LIABILITY FOR FRAUD PERPETRATED SHOULD HAVE A CERTAIN CORRELATION -- IN THE VAST MAJORITY OF CIRCUMSTANCES, THE END USER OR CPE OWNER WILL BE IN THE BEST POSITION TO PROTECT AGAINST THE FRAUD AND SHOULD BEAR THE LOSS FOR FRAUD PERPETRATED

A. CPE Fraud

1. End-User Equipment

Traditionally, station owners (i.e., those who control the CPE) have been responsible for common carriage traffic made over their stations, regardless of whether the call was affirmatively authorized or not.[54] There is certainly some logic to this approach.

The CPE owner controls the predicate equipment for carriage and transport of calls. The equipment is located on the customer's premises in space subject to the control of the owner. While it is true that disgruntled employees may improperly use or manipulate that equipment, or that persons on a premises (whether invitees turned bad or petulant step-children) may make calls not affirmatively authorized, it is also true that the premises owner is the only entity that has the potential to control the situation -- either through barring access to the premises or (upon realization of the problem) through some kind of disciplinary action or network access control.

---

[54] NPRM ¶¶ 8, 20.

Were the Commission to eliminate this kind of station owner responsibility (or cap that responsibility)[55] two things would happen: (1) customers would become cavalier regarding who had access to their equipment and how it was used; and (2) some other entity(ies) would be required to assume a financial obligation for predicate conduct over which they had no control and which was clearly identifiable to a given cost-causing party.[56] Neither of these responses would aid or promote fraud control management or prevention. Nor would the result be an appropriate application of sound risk management or liability principles.

Thus, as a general matter, it makes sense to make the owner/operator of station equipment responsible for calls that traverse that equipment directly (e.g., direct-dialed calls or calls made via built-in remote access features).[57] The owner and operator of CPE, as the purchasing entity and the entity with the primary and paramount care, custody and control of the

---

[55]See discussion below regarding caps on customer's liability at 46-48.

[56]In a regulatory environment in which LECs are subject to price cap controls and a market environment bombarded by prospective competitive entry, LECs do not have an unlimited ability to "pass along" to a captive "customer base" (or to include in a rate base) overhead costs that are more appropriately identified to a given customer or category of customers.

[57]U S WEST does not believe that the Commission's jurisdiction would extend to compelling a customer to equip its CPE with "software or other equipment . . . to prevent fraud." NPRM ¶ 26. Rather, the customer's act of doing so (or failure to do so) could be a material fact in determining and assessing the customer's personal and individual (rather than allocated) liability.

equipment, has (and should have) the primary responsibility for its reliability, including fraud prevention.

CPE purchasers should be expected to either pay for fraud control up front (i.e., necessitating, perhaps, a larger initial investment than might be desirable) or should be expected to pay for the fraud if, and when, it occurs after the fact. The protection and responsibility for fraud losses are properly determined to be one of the myriad of costs of doing business for a business. And, to the extent that fraud constitutes a business risk, and is not adequately protected against up front, a business can investigate the possibility of insuring against the risk[58] (just as it insures against other risks).

Manufacturers of CPE, to be sure, have a responsibility to make clear just what kind of latent risks are associated with the equipment they sell.[59] And, some CPE will have greater "fraud penetration" risks than others. Sales personnel of CPE should also be expected to make clear latent fraud risks.[60] But,

---

[58]NPRM ¶ 11.

[59]It is certainly not inappropriate for the Commission to encourage manufacturer participation in fraud prevention fora and industry activities. However, unless the Commission is willing to mandate some kind of minimum fraud prevention "package" to be included in every conceivable piece of CPE sold on the market, the Commission is not in a position to go much beyond the encouragement phase of the process.

[60]U S WEST believes that this is just good business. Our CPE personnel routinely advise customers, both verbally and in print, of the fraud risks associated with the CPE they buy, suggesting additional service(s)/equipment that might aid the customer in reducing or alleviating the risks attendant to the use of the CPE.

assuming adequate and conspicuous warning,[61] the purchasing choice should be left to the customer. That is what competition is all about -- customer choice and customer responsibility.

The attached Appendix D is a document prepared by the TFPC which does an excellent job of discussing the reasons CPE owners/operators are in the best position to control fraud committed via their equipment. While this fraud prevention will, at times, require the dedication of resources to manage the problem, may require the investment of greater capital or expense dollars than originally anticipated, and may require continuing self-education efforts, this is not unreasonable, given the importance of the telecommunications asset. Any company that is investing in computer technology must understand that the efficiencies and productivities associated with that technology do not come without an ongoing operational, maintenance and security price.

The TFPC document also addresses at some length the "responsibilities" of others involved in the manufacture/sale of the CPE, as well as the transport of traffic emanating from that CPE. The TFPC document notes that LECs have a "supporting role" with regard to CPE fraud, and offers certain suggestions with respect to what actions might be taken in that role. For example, the TFPC documents suggests that LECs might:

---

[61] See further discussion about "Duty to Warn," below at 45.

- Conduct wide customer education through bill inserts, addressing end user groups, holding training seminars, etc.

- Evaluate permitted teaming efforts with long distance companies, equipment manufacturers, etc. to educate customers.

- Evaluate all LEC products and services for security concerns before deployment.

- Where tariff telecommunications systems are offered, fulfill the above suggested security functions of manufacturer and consultant, as appropriate.

- Alert their customer contact personnel (business office, repair, sales/service) to the signs of toll fraud, so that these staffs can better support business owners who are victimized.

- Deploy network blocking services (such as International Direct Dial Blocking) and call screening information digits to complement customer equipment restriction strategies and long distance company network monitoring.

- Develop network monitoring capabilities to highlight potential fraud patterns (local hacking, 800, international, etc.) as early as possible.

- Expand centralized fraud bureau support to a seven day/24 hour basis.

- Continue the use of security staffs to support long distance company investigations and customer inquiries.

- Cooperate with law enforcement agencies in education, investigation and prosecution efforts.

- Develop case documentation for federal and local regulators, in support of guidelines allowing timely and responsive security efforts in cases of toll fraud.[62]

---

[62]Appendix D at 3.

U S WEST is proud to say that we currently support customers' fraud prevention efforts through providing many of the supportive activities suggested by the TFPC.[63] Were the Commission to endorse them as appropriate "suggested efforts" for LECs with regard to CPE fraud, we believe most LECs would already meet or exceed the Commission's expectations.[64]

The above discussion is not meant to suggest that there are not situations in which a customer does everything technologically and reasonably possible to control fraud, and fraud occurs. But, in those circumstances, U S WEST believes that, so long as we determine it appropriate for our business, we should be permitted to assert our limitation of liability against such a loss.

---

[63]U S WEST does not agree that the development of "network monitoring capabilities" for services such as 800 and international calling are properly relegated to LECs. See discussion below at 48-50. While LECs should not be discouraged from providing such services, should they desire, they should not be mandated to become the front-line monitoring agents with regard to interLATA, interstate or international fraud.

[64]While U S WEST does not endorse the concept of shared liability (at least not as a result of regulatory compulsion), as is obvious from the above discussion, should the Commission pursue the concept, the TFPC document would provide a reasonable place to start in identifying respective responsibilities. Compare NPRM ¶ 25 ("We note that shared potential liability would require definition of the specific responsibilities of the CPE-owner to secure the equipment or communications system, of the manufacturer to warn of toll fraud risks associated with features of the CPE, and of the carrier to offer detection and prevention programs and educational services.").

2. Payphones

U S WEST encourages private payphone owners to connect to the network via our Public Access Line ("PAL"),[65] but not all COCOT providers do so.[66] But whether they connect to the network via a PAL or not, one thing remains clear: the COCOT is a piece of CPE.

U S WEST sees no good reason to have one rule of fraud liability for the general population of CPE owners and another rule for COCOT providers. Just as the traditional business should be responsible for its PBX (and its fraud vulnerability), so should a COCOT provider be responsible for the vulnerability of its COCOT equipment -- even if it has done all it can with regard to ordering fraud "prevention" services.[67]

For the above reasons, U S WEST would not support the Florida PSC approach to payphone fraud and liability allocation. First, it seeks to impose virtual strict liability on LECs, even

---

[65]That line contains certain "built-in" security features, resembling OLS and BNS.

[66]Some payphone owners have certain intelligence built into the payphone CPE that operates like OLS/BNS. Others connect to the network with vanilla 1FB lines, a fact that U S WEST discovers often after the fact, i.e., when fraud has occurred.

[67]The idea that an entity should be able to go into a high risk business and then demand no risk is disturbing. In light of the fact that neither OLS nor BNS is a guaranteeable product, an entity deciding to be in the COCOT business faces a reasonably predictable and clearly foreseeable risk from fraud. It can either forego entering the business (because the risk is too high) or enter the business knowing the frailties of both the CPE and associated network. But, what it should not be able to do is enter the business and then seek protection from the risk from some other entity. See supra note 13.

for simple errors.[68] Second, it ignores the fact that determining responsibility of an IXC "for charges that are associated with its failure to properly validate calls via the appropriate LEC data base,"[69] is not a matter that can currently be done verifiably.[70] Third, it operates to immunize a payphone owner from liability based on the owner's purchase of two admittedly-imperfect network screening devices.[71] Fourth, it treats as totally immaterial what other kinds of services/ products the payphone owner might have been in a position to secure in order to protect itself (either currently or in the future).[72] In short, the Florida PSC proposal, while superficially "equitable" and a boon to COCOT providers, does not represent a sound risk management resolution of payphone fraud, and is not equitable to all interested parties.

---

[68]Under the Florida PSC proposal as the Commission describes it, if the COCOT owner has subscribed to BNS and OLS and it does not work, "[t]he LEC is responsible for charges that are associated with the failure of the LEC's screening services, and the IXC is responsible for charges that are associated with its failure to properly validate calls via the appropriate LEC data base." NPRM ¶ 27 n.42. Thus, if the service order were written transposing a single number, the LEC would be liable, despite the fact that the erroneous act might not even rise to the level of negligence.

[69]Id.

[70]See supra note 33.

[71]See discussion supra note 44.

[72]See supra note 46.